Attorney Docket No.:04329.2217

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of	)	
	)	
Masue SHIBA et al	)	
	)	
Serial No.: 09/487,483	)	Group Art Unit: 2766
	)	
Filed: January 19, 2000	)	Examiner: Not Assigned

For: ARITHMETIC METHOD AND APPARATUS
AND CRYPTO PROCESSING APPARATUS

CLAIM FOR PRIORITY

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Under the provisions of 35 U.S.C. § 119, Applicants hereby claim the benefit of the filing date of Japanese Patent Application Nos. 11-011989, filed on January 20, 1999 and 11-209831, filed on July 23, 1999, for the above-identified U.S. patent application.

In support of Applicants' claim for priority, filed herewith are certified copies of the above.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

By: _____
Richard V. Burgujian
Reg. No. 31,744
ERNEST F. CHAPMAN
Reg. No. 25,961

Dated: May 1, 2000
RVB/FPD/sci
Enclosure

LAW OFFICES
FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, D. C. 20005
202-408-4000

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

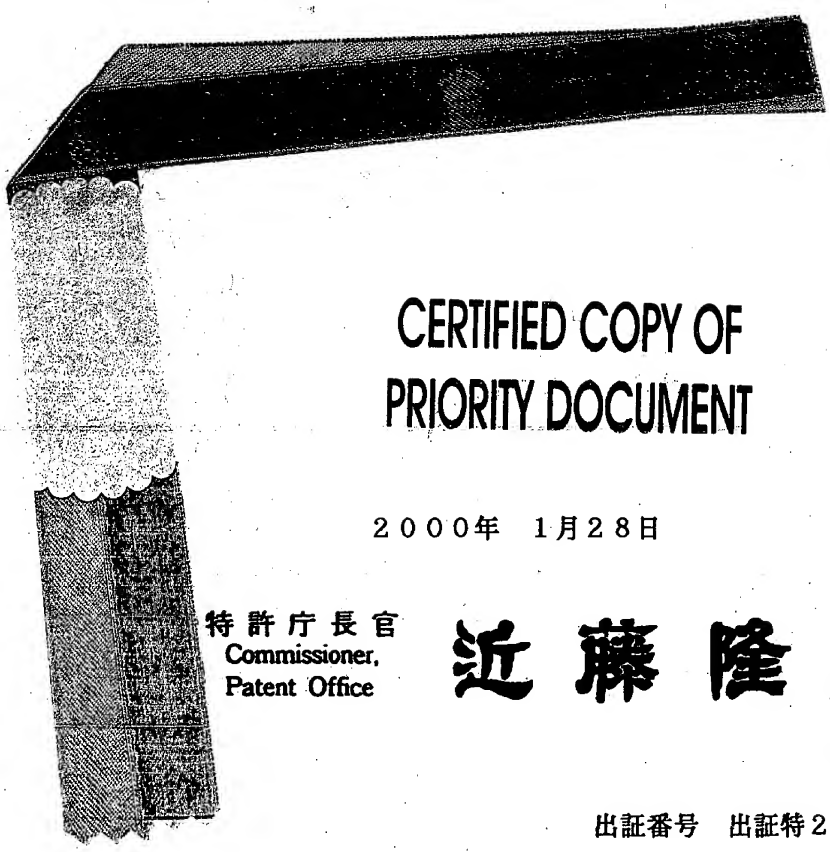
別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: １９９９年　１月２０日

出 願 番 号
Application Number: 平成１１年特許願第０１１９８９号

出 願 人
Applicant (s): 株式会社東芝



CERTIFIED COPY OF
PRIORITY DOCUMENT

２０００年　１月２８日

特許庁長官
Commissioner,
Patent Office 近藤隆彦

出証番号　出証特２０００－３００１１５８

【書類名】　特許願

【整理番号】　A009807708

【提出日】　平成11年 1月20日

【あて先】　特許庁長官　殿

【国際特許分類】　G06F　7/00

【発明の名称】　演算装置及び暗号処理装置

【請求項の数】　7

【発明者】

【住所又は居所】　東京都府中市東芝町１番地　株式会社東芝府中工場内

【氏名】　斯波　万恵

【発明者】

【住所又は居所】　東京都府中市東芝町１番地　株式会社東芝府中工場内

【氏名】　川村　信一

【特許出願人】

【識別番号】　000003078

【氏名又は名称】　株式会社　東芝

【代理人】

【識別番号】　100058479

【弁理士】

【氏名又は名称】　鈴江　武彦

【電話番号】　03-3502-3181

【選任した代理人】

【識別番号】　100084618

【弁理士】

【氏名又は名称】　村松　貞男

【選任した代理人】

【識別番号】　100068814

【弁理士】

【氏名又は名称】　坪井　淳

【選任した代理人】

【識別番号】　100092196

【弁理士】

【氏名又は名称】　橋本　良郎

【選任した代理人】

【識別番号】　100091351

【弁理士】

【氏名又は名称】　河野　哲

【選任した代理人】

【識別番号】　100088683

【弁理士】

【氏名又は名称】　中村　誠

【選任した代理人】

【識別番号】　100070437

【弁理士】

【氏名又は名称】　河井　将次

【手数料の表示】

【予納台帳番号】　011567

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　演算装置及び暗号処理装置

【特許請求の範囲】

【請求項１】　多倍長の積和演算装置であって、

整数型の単位乗算を実行する場合にはキャリーを伝搬させて単位乗算回路を動作させ、２の拡大体の単位乗算を実行する場合にはキャリーを伝搬させずに単位乗算回路を動作させるようにしたことを特徴とする演算装置。

【請求項２】　少なくとも整数型の単位乗算回路を含んで構成される多倍長整数の積和演算装置であって、

前記整数型の単位乗算回路と論理的に隣接して配置された２の拡大体の単位乗算回路と、

前記整数型の単位乗算回路を使用するか、前記２の拡大体の単位乗算回路を使用するかを選択する選択手段と

を備えたことを特徴とする演算装置。

【請求項３】　少なくとも整数型の単位乗算回路を含んで構成される多倍長整数の積和演算装置であって、

整数型の単位乗算を実行するか、２の拡大体の単位乗算を実行するかの選択信号を前記整数型の単位乗算回路に出力する制御手段を備えるとともに、

前記整数型の単位乗算回路は、多倍長の積和演算を実行する際に、整数型の単位乗算を実行すべき旨の選択信号を受けたときにはキャリーを伝播し、２の拡大体の単位乗算を実行すべき旨の選択信号を受けたときにはキャリー伝搬をしないキャリー伝搬制御手段を備え、

前記単位乗算回路におけるキャリー伝搬を制御することにより、整数型乗算と２の拡大体の乗算を切替可能に構成されたことを特徴とする演算装置。

【請求項４】　請求項３の演算装置において、

前記キャリー伝搬制御手段は、前記選択信号とキャリーアウト信号を入力とするスイッチによって、１ビット毎の全加算器におけるキャリーの伝搬制御を行うことを特徴とする演算装置。

【請求項５】　請求項３の演算装置において、

前記キャリー伝搬制御手段は、１ビット毎の全加算器における２入力ａ，ｂの排他的論理和の結果ｃを加算結果として出力するか、前記結果ｃと入力キャリーとの排他的論理和の結果ｄを加算結果として出力するかを切り替える選択手段からなることを特徴とする演算装置。

【請求項６】　請求項１乃至５のうち何れか１項に記載の演算装置において、

前記整数型の乗算を実行する場合にはキャリーを伝搬させて加算を実行し、２の拡大体の乗算を実行する場合にはキャリーを伝搬させずに加算を実行する加算回路を備えたことを特徴とする演算装置。

【請求項７】　請求項１乃至６のうち何れか１項に記載の演算装置を備え、

前記演算装置による整数型の演算に基づく暗号化又は復号処理と、前記演算装置による２の拡大体の演算に基づく暗号化又は復号処理との双方を切替可能に構成されたことを特徴とする暗号処理装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

この発明は演算装置及び暗号処理装置、特に例えばＩＣカードに実装される暗号処理用コプロセッサ等に用いるのに適した演算装置及び暗号処理装置に関するものである。

【０００２】

【従来の技術】

公開鍵暗号のＬＳＩ実装においては、従来からＲＳＡ方式等の整数型の演算を行う暗号方式が主に採用されている。この方式では、桁数の大きい整数についての演算を行う必要があるため、ＩＣカード等に応用する場合には専用コプロセッサが必要とされる。このような専用コプロセッサを実装して暗号処理の多倍長整数演算を実現させる方式については既に多数の実績がある。

【０００３】

一方、近年整数型ではなく、２の拡大体（ＧＦ（２＾ｍ）：Ｇａｌｏｉｓ　Ｆｉｅｌｄ（ガロアフィールド））といわれる代数系の上で構成される暗号系，特

に２の拡大体の楕円暗号方式が注目されている。

【０００４】

この２の拡大体演算を用いる暗号方式においても、ＲＳＡ方式等の整数型の演算の方式の同様に、扱うビット数を１６０ビット以上と大きくとる必要がある。このため、ＩＣカードのようなＣＰＵの演算力が低い装置上でこれを実現しようとすると比較的処理時間がかかる。したがって、専用のハードウェア（コプロセッサ）を用いて高速化したいという要求がある。

【０００５】

このようにＲＳＡ方式であっても、楕円暗号方式であっても、ＩＣカード等において高速な暗号処理を実現させるためには専用の演算用コプロセッサを用意する必要がある。

【０００６】

図１０は暗号処理用のコプロセッサを含むＩＣカード用ＬＳＩのブロック図である。

【０００７】

同図に示す構成要素を含む専用ＬＳＩが例えばＩＣカードに組み込まれる。このＬＳＩにおいては、ＣＰＵ、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭが１チップに収容され、コプロセッサはＲＡＭ、演算部、制御部から構成される。コプロセッサはＣＰＵの制御下にあって多倍長のべき乗剰余演算や四則演算といった公開鍵暗号の基本演算に関しＣＰＵを補助する。つまり、暗号の基本演算を行う部分は図１０におけるコプロセッサであり、この部分がどのように構成されているかが問題となる。

【０００８】

図１１は図１０に示すＬＳＩにおけるコプロセッサ部分の構成例を示すブロック図である。

【０００９】

ＲＳＡ方式では整数型の演算が行われるため、このコプロセッサは図１１に示すように整数型の乗算器として構成されている。

【００１０】

一方、楕円暗号方式のＬＳＩを作成する場合、その全体的な構成は図１０に示すＬＳＩと同様あるいはこれと類似する構成のものとなるが、コプロセッサ部分における演算は整数型の演算でなく、２の拡大体演算を行うコプロセッサを用意する必要がある。

【００１１】

図１２は多項式基底の２の拡大体演算を行うコプロセッサのハードウェア構成例を示すブロック図である。

【００１２】

同図は、「楕円暗号のハードウェア実装，ＳＣＩＳ’９８－１０．１．Ｃ」にて発表された特殊な既約多項式を用いる円分体といわれる２の拡大体の一種の演算装置を示している。この演算装置は、２の拡大体上の加算、二乗、乗算及び逆元演算を実行できる構成を備えており、これによって楕円曲線上の点の演算に必要な２の拡大体の演算を実行する。このような演算装置をＩＣ化すれば、図１０のＬＳＩに適用し得る２の拡大体演算用のコプロセッサになる。

【００１３】

ここで、加算回路および二乗算回路はｍ個のＥＸ－ＯＲで構成され、乗算回路８１は図１３に示す回路構成で実現する。

【００１４】

図１３は円分体といわれる２の拡大体の乗算回路を示す図である。

【００１５】

この乗算回路８１は、ｍビットの入力レジスタＡ，Ｂを持ち多項式ａ（ｘ）の係数を入力レジスタＡに固定値として入力し、入力レジスタＢからは多項式ｂ（ｘ）の係数を最上位ビットから１クロック毎にシフトしながら演算していく。同図におけるブロックＤはフィードバックレジスタを構成するフリップフロップである。ｍ回シフトした時点での各ブロックＤの値が出力レジスタＣに読み出され、ａ（ｘ）＊ｂ（ｘ）の演算結果となる。

【００１６】

図１１と図１３夫々の回路を見比べてもわかるように、乗算と一口に言っても整数型乗算と多項式基底の２の拡大体乗算とでは、その乗算を実行するためのア

ーキテクチャーが全く異なる。したがって、従来は暗号方式毎にハードウェアを構成しようとする試みがなされてきた。

【００１７】

【発明が解決しようとする課題】

上記したように、楕円暗号方式は現在注目されてはいるものの、現状ではＲＳＡ暗号方式が未だ主流であるため、楕円暗号方式を用いるＩＣカードにおいてもＲＳＡ暗号にも対応させたいという要請が強い。

【００１８】

ここで、従来の整数型の暗号と２の拡大体の暗号を同一ＩＣカードに実装しようとした場合、上記した従来技術の延長ではそれぞれに対応するコプロセッサを搭載する必要が生じる。しかしながら、２つのコプロセッサを搭載したのでは、面積制約の大きいＩＣカードにおいてそのチップ面積を圧迫するという問題が生じる。

【００１９】

本発明は、このような実情を考慮してなされたもので、最小のアーキテクチャを追加するだけで整数型の演算に加えて２の拡大体上の演算をも実行できる演算装置及び暗号処理装置を提供することを目的とする。

【００２０】

【課題を解決するための手段】

上記課題を解決するために、請求項１に対応する発明は、多倍長の積和演算装置であって、整数型の単位乗算を実行する場合にはキャリーを伝搬させて単位乗算回路を動作させ、２の拡大体の単位乗算を実行する場合にはキャリーを伝搬させずに単位乗算回路を動作させるようにした演算装置である。

【００２１】

本発明はこのような手段を設けたので、最小のアーキテクチャを追加するだけで整数型の演算に加えて２の拡大体上の演算をも実行することができる。

【００２２】

次に、請求項２に対応する発明は、少なくとも整数型の単位乗算回路を含んで構成される多倍長整数の積和演算装置であって、整数型の単位乗算回路と論理的

に隣接して配置された２の拡大体の単位乗算回路と、整数型の単位乗算回路を使用するか、２の拡大体の単位乗算回路を使用するかを選択する選択手段とを備えた演算装置である。

【００２３】

本発明はこのような手段を設けたので、２の拡大体の単位乗算回路を追加するだけで整数型の乗算と２の拡大体の乗算の双方を実行することができる。

【００２４】

次に、請求項３に対応する発明は、少なくとも整数型の単位乗算回路を含んで構成される多倍長整数の積和演算装置であって、整数型の単位乗算を実行するか、２の拡大体の単位乗算を実行するかの選択信号を整数型の単位乗算回路に出力する制御手段を備えるとともに、整数型の単位乗算回路は、多倍長の積和演算を実行する際に、整数型の単位乗算を実行すべき旨の選択信号を受けたときにはキャリーを伝播し、２の拡大体の単位乗算を実行すべき旨の選択信号を受けたときにはキャリー伝搬をしないキャリー伝搬制御手段を備え、単位乗算回路におけるキャリー伝搬を制御することにより、整数型乗算と２の拡大体の乗算を切替可能に構成された演算装置である。

【００２５】

本発明はこのような手段を設けたので、キャリー伝搬制御手段を追加するだけで整数型の乗算と２の拡大体の乗算の双方を実行することができる。

【００２６】

次に、請求項４に対応する発明は、請求項３の演算装置において、キャリー伝搬制御手段は、選択信号とキャリーアウト信号を入力とするスイッチによって、１ビット毎の全加算器におけるキャリーの伝搬制御を行う演算装置である。

【００２７】

本発明はこのような手段を設けたので、選択信号とキャリーアウト信号を入力とするスイッチにより請求項３に係る発明を実現させることができる。

【００２８】

次に、請求項５に対応する発明は、請求項３の演算装置において、キャリー伝搬制御手段は、１ビット毎の全加算器における２入力ａ，ｂの排他的論理和の結

果ｃを加算結果として出力するか、結果ｃと入力キャリーとの排他的論理和の結果ｄを加算結果として出力するかを切り替える選択手段からなる演算装置である。

【００２９】

本発明はこのような手段を設けたので、選択手段により請求項３に係る発明を実現させることができる。

【００３０】

次に、請求項６に対応する発明は、請求項１～５の演算装置において、整数型の乗算を実行する場合にはキャリーを伝搬させて加算を実行し、２の拡大体の乗算を実行する場合にはキャリーを伝搬させずに加算を実行する加算回路を備えた演算装置である。

【００３１】

本発明はこのような手段を設けたので、積和演算における加算部分についても整数型の乗算と２の拡大体の乗算との双方を確実に実行することができる。

【００３２】

次に、請求項７に対応する発明は、請求項１～６の何れかの演算装置を備え、演算装置による整数型の演算に基づく暗号化又は復号処理と、演算装置による２の拡大体の演算に基づく暗号化又は復号処理との双方を切替可能に構成された暗号処理装置である。

【００３３】

本発明はこのような手段を設けたので、ＲＳＡ暗号等の整数型の演算に基づく暗号と、楕円曲線暗号等の２の拡大体の演算に基づく暗号の双方の処理を行うことができる。

【００３４】

【発明の実施の形態】

以下、本発明の実施の形態について説明する。

（発明の第１の実施の形態）

図１は本発明の第１の実施形態に係る演算装置の構成例を示すブロック図である。

【００３５】

コプロセッサ１として構成される本実施形態の演算装置は、整数型乗算及び２の拡大体乗算の双方の演算が可能な多倍長積和乗算装置であり、この乗算処理を仕方を制御することにより、加算、二乗あるいは逆元等の他の演算を実行するものである。また、本演算装置がＬＳＩ等に組み込まれることによってＲＳＡ暗号及び楕円暗号の双方が実現可能な暗号処理装置が構成される。ここで組込対象となるＬＳＩは例えば図１０に示すような装置である。

【００３６】

このコプロセッサ１において演算部４は制御部５によってコントロールされ、演算途中のデータを格納するメモリ２から接続される３２ビットのデータバス３からデータを入出力するようになっている。

【００３７】

データバス３からの入力データはバッファＺ，Ｙ，Ｘに格納され、データバス３への出力データはバッファＲに格納されるようになっている。

【００３８】

入力データＸ及びＹは乗算対象となるデータであり、このうちデータＹは一度に多数桁の乗算となるのを回避するために所定桁毎に分割されたデータとして入力される。一方、データＺは乗算を複数回に分けて実行するために生じる途中結果であり、これをＸＹの乗算結果に足し、さらにその和の結果にキャリーＣと言われる桁上がり部分を足して１サイクルの乗算が終了する。その結果からキャリーを除いたデータＲがバッファＲを介してデータバス３に出力され、次のサイクルの演算にデータＺとして使用される。このサイクルを複数回繰り返すことにより多倍長整数乗算あるいは２の拡大体乗算（厳密には後述のｃ’）の乗算が実現される。

【００３９】

また、コプロセッサ１は、上記演算を実現するために、バッファＸ，Ｙ，Ｚ，Ｒの他、整数型乗算回路１１，２の拡大体上乗算回路１２，セレクタ１３，加算回路１４，加算回路１５，キャリー保持部１６及び制御部５を備えている。

【００４０】

整数型乗算回路１１は、バッファＸ内のデータＸとバッファＹ内のデータＹとを整数型乗算し、その結果をセレクタ１３に出力する。

【００４１】

２の拡大体上乗算回路１２は、バッファＸ内のデータＸとバッファＹ内のデータＹとにより２の拡大体上乗算の一部（ｃ’）を実行し、その結果をセレクタ１３に出力する。

【００４２】

セレクタ１３は、制御部５からの信号Ｓ１に従って、整数型乗算回路１１又は２の拡大体上乗算回路１２からの出力の何れかを加算回路１４に出にする。

【００４３】

加算回路１４は全加算器からなり、バッファＺ内のデータＺとセレクタ出力を加算して加算回路１５に出力する。この加算回路１４においては、整数型の加算と２の拡大体の加算との切替が制御信号Ｓ１に従って行われるようになっている。なお、この加算切替については後述する。

【００４４】

加算回路１５は、加算回路１４の出力にキャリー保持部１６に保持されたキャリーＣを加算し上位３２ビットを次のキャリーＣとしてキャリー保持部１６に出力し、下位８ビットをこのサイクルの演算結果であるデータＲをとしてバッファＲに出力する。なお、加算回路１５においても、制御信号Ｓ１により、整数型の加算と２の拡大体の加算との切替が行われるようになっている。

【００４５】

キャリー保持部１６は、加算回路１５から出力されたキャリーＣを保持し、次の演算サイクルにおいて保持したキャリーＣを加算回路１５に与える。

【００４６】

制御部５は、整数演算制御部２１と２の拡大体演算制御部２２からなり、これらの何れかのコマンド群に従って演算部を制御する。このコマンド切り替えは、外部のＣＰＵ（例えば図１０に示すＣＰＵ）からの指示によって行われる。

【００４７】

整数演算制御部２１は、演算部４を多倍長整数演算型の乗算器として動作する

ように制御するものである。このために、制御信号Ｓ１によりセレクタ１３が整数型単精度乗算器１１の出力を加算回路１４に出力するように制御するとともに、加算回路１４及び１５を整数型加算回路として動作するよう制御する。さらに、整数型乗算器として演算部４の動作を制御することで他の四則演算などの演算処理の実行する。

【００４８】

また、２の拡大体演算制御部２２は、演算部４を２の拡大体乗算器として動作するように制御するものである。このために、制御信号Ｓ１によりセレクタ１３が２の拡大体型単精度乗算器１１の出力を加算回路１４に出力するように制御するとともに、加算回路１４及び１５を２の拡大体型加算回路として動作するように制御する。さらに、２の拡大体型乗算器として演算部４の動作を制御することで加算、二乗算を実現する。

【００４９】

なお、制御部５からは、上記した各処理を実現するため、制御信号Ｓ２を出力して各部を制御する。

【００５０】

次に、以上のように構成された本実施形態における演算装置の動作について説明する。

【００５１】

この演算装置（コプロセッサ１）は、整数型の乗算装置に乗算回路１２，セレクタ１３等を組み込むことにより、２の拡大体の乗算装置としての処理を実現可能とするものであるがある。ここで、２の拡大体では、以下に示すようにｍ－１次の多項式をｍビットのベクトル表現で表すことができる。

【００５２】

$$a(x) = a_{m-1}x^{(m-1)} + a_{m-2}x^{(m-2)} + \cdots + a_1x + a_0 \quad \cdots (1)$$
$$= [a_{m-1}, \cdots, a_1, a_0]$$

ここで、２の拡大体の乗算はＧＦ（２）上のｍ次の規約多項式ｇ（ｘ）をモジュラスとする剰余乗算である。また、２の拡大体の二つの元ａ（ｘ）とｂ（ｘ）の積ｃ（ｘ）は、次のように定義されている。

【００５３】

$$c(x)=a(x)*b(x) \bmod g(x) \quad \cdots(2)$$

$$=\Sigma a_k * x^k * b(x) \bmod g(x)$$

２の拡大体の多項式の乗算は、図１３に示すように乗数のサイクルシフトによるシフトレジスタを構成し、ｍサイクルシフト後の剰余多項式を乗算結果とするのが一般的であるが、本実施形態では整数型の暗号処理ＬＳＩで広く使われている多倍長の積和演算回路に若干の変更を加えて処理する。

【００５４】

なお、制御部５からの制御信号Ｓ１により、コプロセッサ１が整数型の演算装置として動作するときには、同演算装置は多倍長積和演算回路として機能している。この多倍長積和演算回路において、制御信号Ｓ１による切替により、２の拡大体上乗算回路１２において２の拡大体の乗算の一部分である（３）式が計算される。

【００５５】

$$c'(x)=a(x)*b(x) \quad \cdots(3)$$

なお、２の拡大体上乗算回路１２ではｃ’を計算する段階においては（２）式における「ｃ（ｘ）’ｍｏｄ　ｇ（ｘ）」の部分は計算されない。すなわちｃ’自体は、制御信号Ｓ１により乗算回路１２及び加算回路１４，１５を切り替えるのみで、整数型乗算における２つの数の積と全く同様に演算される。

【００５６】

なお、ｃ’（ｘ）＝ａ（ｘ）＊ｂ（ｘ）においてｍビットの乗数、被乗数は３２ビットに分割されてメモリから読み出され、演算結果は３２ビット毎にメモリに書き込まれる。この時、最終的な演算結果は２ｍビットとなる。

【００５７】

整数型乗算回路１１による整数演算と２の拡大体上乗算回路１２による２の拡大体多項式演算の違いは、桁上がりの有無である。整数演算では足し算の論理式は

０＋０＋Ｃａｒｒｙ（＝０）＝０、Ｃａｒｒｙ＝０

１＋０＋Ｃａｒｒｙ（＝０）＝１、Ｃａｒｒｙ＝０

１＋１＋Ｃａｒｒｙ（＝０）＝０、Ｃａｒｒｙ＝１

という様に下位ビットのキャリーを考慮した演算をしなければならないのに対し、２の拡大体の代数系においては、各ビットが多項式における次数の係数を示しているため異なる次数への桁上がりを考慮しなくてもよい。

【００５８】

このことに着目して本実施形態では整数型演算器（乗算器や加算器）において、キャリー伝播を許す通常のモードと、キャリー伝播を実行しないモードを切り替えて使えるようにしているのである。ここでキャリー伝播を許さない（実行しない）モードは２の拡大体演算を行うのに用いられる。なお、キャリー伝播のモードを切り替えのために追加すべき回路は全体の回路規模に比べわずかである。

【００５９】

図２はｃ’（ｘ）＝ａ（ｘ）＊ｂ（ｘ）を実現するための４＊４ビットの単位乗算の回路構成例を示す図である。

【００６０】

同図の単位演算装置を８＊３２ビット構成にしたものが図１における２の拡大体上乗算回路１２である。なお、図２（ｂ）の回路は同図（ａ）の回路の入力部分２９を示すものである。

【００６１】

一方、図３は整数型乗算を実現するための４＊４ビットの単位乗算の回路構成例を示す図である。

【００６２】

同図の単位演算装置を８＊３２ビット構成にしたものが図１における整数型乗算回路１１である。なお、図３（ａ）に用いられる全加算器ＦＡの構成は図３（ｃ）に示され、さらに図３（ｃ）に示す全加算器ＦＡのキャリー３１の構成が同図（ｄ）に示されている。また、図３（ｂ）の回路は同図（ａ）の回路の入力部分３０を示すものである。

【００６３】

本実施形態の演算装置では、２の拡大体上乗算回路１２と整数型乗算回路１１とが論理的に隣接して配置されており、制御部５の２の拡大体演算コマンドから

生成される制御信号Ｓ１により整数型、２の拡大体型のいずれかの乗算回路１１，１２が選択されて処理が行われる。

【００６４】

セレクタ１３の出力は次段の加算回路１４に入力される。ここでＺ＋（Ｙ＊Ｘ）加算回路１４は４０ビットのデータ（Ｙ＊Ｘ）と８ビットのデータＺの全加算器だが、ここでも前述の制御信号により各ビットの加算結果のキャリーを次段へ伝播しないスイッチを付加することにより２の拡大体の加算が実現される。

【００６５】

図４は本実施形態におけるコプロセッサに用いられるキャリー制御機能付きの４ビットのリップルキャリー型全加算器の構成例を示すブロック図である。

【００６６】

このような構成の全加算器を、４０ビットデータと８ビットデータとの加算が可能となるように拡張したものが図１の加算回路１４である。

【００６７】

また、図４の回路において、各全加算器３２の間にはスイッチ３３が設けられ、キャリーの伝搬を制御できるようになっている。

【００６８】

図５は本実施形態の加算回路に用いられる全加算器及びキャリー制御スイッチの構成例を示す図である。

【００６９】

この全加算器３２及びスイッチ３３は、１ビット分のキャリー制御機能付き全加算器４２を構成している。ここで、全加算器３２は、図３（ｃ）に示す全加算器ＦＡと同様に構成され、全加算器３２内のキャリー３１は図３（ｄ）に示すキャリーと同様に構成されている。

【００７０】

また、全加算器３２間のキャリー伝搬ラインに設けられたスイッチ３３は制御部５からの制御信号Ｓ１によって制御され、整数型演算を行うときには接続され、２の拡大体演算を行うときには遮断される。

【００７１】

以上のように構成された加算回路１４からの出力（Ｚ＋（Ｙ＊Ｘ））は加算回路１５に引き渡される。

【００７２】

すなわち、演算ブロック最終段のＣ＋Ｚ＋（Ｙ＊Ｘ）加算回路１５によって、乗算結果の４０ビットの下位８ビットがデータＲとして出力され、上位３２ビットが次のサイクルのＺ＋（Ｙ＊Ｘ）に足し込まれる。

【００７３】

ここで、加算回路１５は加算回路１４と同様に、前述の制御信号Ｓ１により制御される図４に示すキャリー制御機能付き全加算器であるので、整数型ではＬＳＢに桁あわせをした全加算器として整数型加算が実行され、２の拡大体演算では２の拡大体加算が実行される。

【００７４】

加算回路１５の出力データＲはデータバス３を介して一旦外部のメモリ２に出力され、再びデータＺとなってコプロセッサ１内に戻り整数型乗算若しくは２の拡大体上の乗算が継続され、必要なサイクル数だけ繰り返されて乗算結果が得られる。

【００７５】

ここで２の拡大体の乗算コマンドでは、（２）式の結果が得られるが、２の拡大体乗算は（３）式に示す定義通り、既約多項式ｇ（ｘ）をモジュラスとする剰余演算によって完結する。剰余演算は割り算の筆算同様、被除数の上位桁から商を立て現在の商と除数をかけたものから現在の被除数を引く（２の拡大体では減算は加算と同じ）処理を必要なサイクル数だけ繰り返せばよく、２の拡大体の乗算コマンドと加算コマンドを実行することによって実現できる。２の拡大体の二乗算は乗算と同じ処理で実現でき、逆元計算は、乗算と二乗算を相互に繰り返すことにより実現できる。

【００７６】

一例として、２の拡大体の加算コマンドに従って演算部４が２の拡大体の加算装置として機能する場合を説明する。

【００７７】

２の拡大体上の加算は、通常の多項式の加算と同じで、同じ次数の係数同士の足し算を行う。

【００７８】

$$c(x)=a(x)+b(x) \qquad \cdots(4)$$

$$=[a_{m-1}+b_{m-1},\ a_{m-2}+b_{m-2},\ \cdots,\ a_0+b_0]$$

このとき、各次数の係数の和は０＋０＝１＋１＝０、０＋１＝１＋０＝１となり、整数型加算のようにキャリーは発生しない。従って、２の拡大体での加算は、一般にはｍ個のＥＸ－ＯＲで実装できることになる。

【００７９】

整数型の乗算装置において加算はｃ＝ｂ＋ａ＊１として扱えるので、本実施形態における２の拡大体の加算もこのアルゴリズムをそのまま利用し、ｃ（ｘ）＝ｂ（ｘ）＋ａ（ｘ）＊１として実行する。この演算は加算回路１４，１５に図４の全加算器が用いられていることから、制御信号Ｓ１の切替で実現できる。

【００８０】

また、制御信号Ｓ１による切替でコプロセッサ１は図１１に示すコプロセッサと同様な機能を持つ回路となり、整数型演算も実現される。

【００８１】

上述したように、本発明の実施の形態に係る演算装置は、整数型乗算装置に、整数型乗算の単位乗算装置と回路構成の似ている２の拡大体乗算の単位演算装置とを設け、整数型の乗算コマンドに２の拡大体演算コマンドとを追加し、２の拡大体演算コマンドから生成される制御信号により制御されるセレクタと、全加算器の各ビットのキャリーの伝播を制御するスイッチの追加するようにしたので、従来型のシフトレジスタによるシーケンシャルな２の拡大体の乗算装置を用いることなく整数および２の拡大体演算の両方を実行することができる。

【００８２】

したがって、従来からある整数型の演算器への追加拡張機能として、ごく少ない命令と回路の追加することにより、多倍長の積和演算回路で２の拡大体の加算、乗算を実行することが可能な公開鍵暗号処理用アクセラレータを提供することができる。なお、本実施形態を実現するのに、必要な回路追加の量は全体の回路

規模に比べてわずかである。

【００８３】

本実施形態の暗号処理装置によれば、暗号処理用コプロセッサとして、整数型のＲＳＡ方式に加え２の拡大体の楕円暗号方式も処理できる豊富な機能をもつＬＳＩを特に実装面積を増大させることなく提供できる。したがって、ＩＣカードのような実装可能面積の少ない装置において、ＲＳＡ、楕円暗号の双方を処理できる暗復号装置を実現させることができる。

（変形例１）

本変形例では、図４に示す加算回路１４，１５を構成するキャリー制御機能付き全加算器について説明する。

【００８４】

図６はキャリー制御機能付き全加算器の変形例を示す図である。

【００８５】

このキャリー制御機能付き全加算器４３は、スイッチ３３と全加算器３２から構成される点で図５の回路と共通する。しかし、図５の回路ではキャリー３１の出力側にスイッチ３３が設けられているのに対し、図６の回路ではキャリー３１の入力側にスイッチ３３が設けられている。

（変形例２）

本変形例では、更に他のキャリー制御機能付き全加算器について説明する。

【００８６】

図７はキャリー制御機能付き全加算器の他の変形例を示す図である。

【００８７】

このキャリー制御機能付き全加算器４４は、加算結果の出力選択を制御することによりキャリー制御を行う。すなわちスイッチ３３’はセレクタで構成され、このセレクタは制御信号Ｓ１に基づき、ＥＸＯＲ３５又はＥＸＯＲ３６の出力を選択する。これを複数個連結したリップルキャリー型加算器は、制御信号Ｓ１によりキャリー伝播の有無を制御できる。

【００８８】

図７の制御信号Ｓ１を２の拡大体演算コマンドによる制御信号とするとＳ１が

“１”のときａとｂのＥＸＯＲ３５の出力が演算結果となり、２の拡大体の加算装置として機能し、Ｓ１が“０”のとき全加算器の出力が演算結果となって整数型の加算装置として機能する。

（発明の第２の実施の形態）

図８は本発明の第２の実施形態に係る演算装置の構成例を示すブロック図であり、図１と同一部分には同一符号を付して説明を省略し、ここでは異なる部分についてのみ述べる。

【００８９】

この演算装置であるコプロセッサ１’は、図１における整数型乗算回路１１，２の拡大体上乗算回路１２及びセレクタ１３に代えて乗算回路４１を備える他、第１の実施形態と同様に構成されている。

【００９０】

この乗算回路４１は、制御部５からの制御信号Ｓ１によって整数型乗算と２の拡大体上乗算（（３）式のｃ’のみ）を切り替えるようになっている。

【００９１】

図９は本実施形態の乗算回路を実現するための４＊４ビットの単位乗算の回路構成例を示す図である。なお、現実の乗算回路４１は、同図の単位演算装置を８＊３２ビット構成にしたものである。また、図９（ｂ）の回路は同図（ａ）の回路の入力部分２９を示すものである。

【００９２】

この乗算回路４１は、図９（ａ）に示すように、全加算器として図５に示すキャリー制御機能付き全加算器４２を用いているので、制御信号Ｓ１に従ってキャリー伝搬の有無を制御できる。したがって、２の拡大体演算コマンドによる整数型乗算と２の拡大体上乗算との切替が実現される。

【００９３】

こうして本実施形態の演算装置では第１の実施形態と同様な動作が実現される。

【００９４】

上述したように、本発明の実施の形態に係る演算装置及び暗号処理装置は、整

数型乗算回路１１，２の拡大体上乗算回路１２及びセレクタ１３に代えて乗算回路４１を用いるようにし、一つの回路４１で回路１１，１２及び１３の機能を実現するようにしたので、第１の実施形態と同様な効果が得られる他、より少ない回路追加で整数型乗算と２の拡大体上乗算との切り替えを実現にすることができる。

【００９５】

なお、本実施形態ではキャリー制御機能付き全加算器４２として図５に示すものを用いるようにしたが、キャリー制御機能付き全加算器４２に代えて、図６又は図７に示すキャリー制御機能付き全加算器４３又は４４を用いるようにしてもよい。

【００９６】

【発明の効果】

以上詳記したように本発明によれば、最小のアーキテクチャを追加するだけで整数型の演算に加えて２の拡大体上の演算をも実行できる演算装置及び暗号処理装置を提供することができる。

【図面の簡単な説明】

【図１】

本発明の第１の実施形態に係る演算装置の構成例を示すブロック図。

【図２】

ｃ’（ｘ）＝ａ（ｘ）＊ｂ（ｘ）を実現するための４＊４ビットの単位乗算の回路構成例を示す図。

【図３】

整数型乗算を実現するための４＊４ビットの単位乗算の回路構成例を示す図。

【図４】

同実施形態におけるコプロセッサに用いられるキャリー制御機能付きの４ビットのリップルキャリー型全加算器の構成例を示すブロック図。

【図５】

同実施形態の加算回路に用いられる全加算器及びキャリー制御スイッチの構成例を示す図。

【図６】

キャリー制御機能付き全加算器の変形例を示す図。

【図７】

キャリー制御機能付き全加算器の他の変形例を示す図。

【図８】

本発明の第２の実施形態に係る演算装置の構成例を示すブロック図。

【図９】

同実施形態の乗算回路を実現するための４＊４ビットの単位乗算の回路構成例を示す図。

【図１０】

暗号処理用演算用コプロセッサを含むＩＣカード用ＬＳＩのブロック図。

【図１１】

図１０に示すＬＳＩにおけるコプロセッサ部分の構成例を示すブロック図。

【図１２】

多項式基底の２の拡大体演算を行うコプロセッサのハードウェア構成例を示すブロック図。

【図１３】

円分体といわれる２の拡大体の乗算回路を示す図。

【符号の説明】

１，１’…コプロセッサ

２…メモリ

３…データバス

１１…整数型乗算回路

１２…２の拡大体上乗算回路

１３…セレクタ

１４…加算回路

１５…加算回路

１６…キャリー保持部

２１…整数演算制御部

２２…２の拡大体演算制御部

３２…全加算器

３３…スイッチ

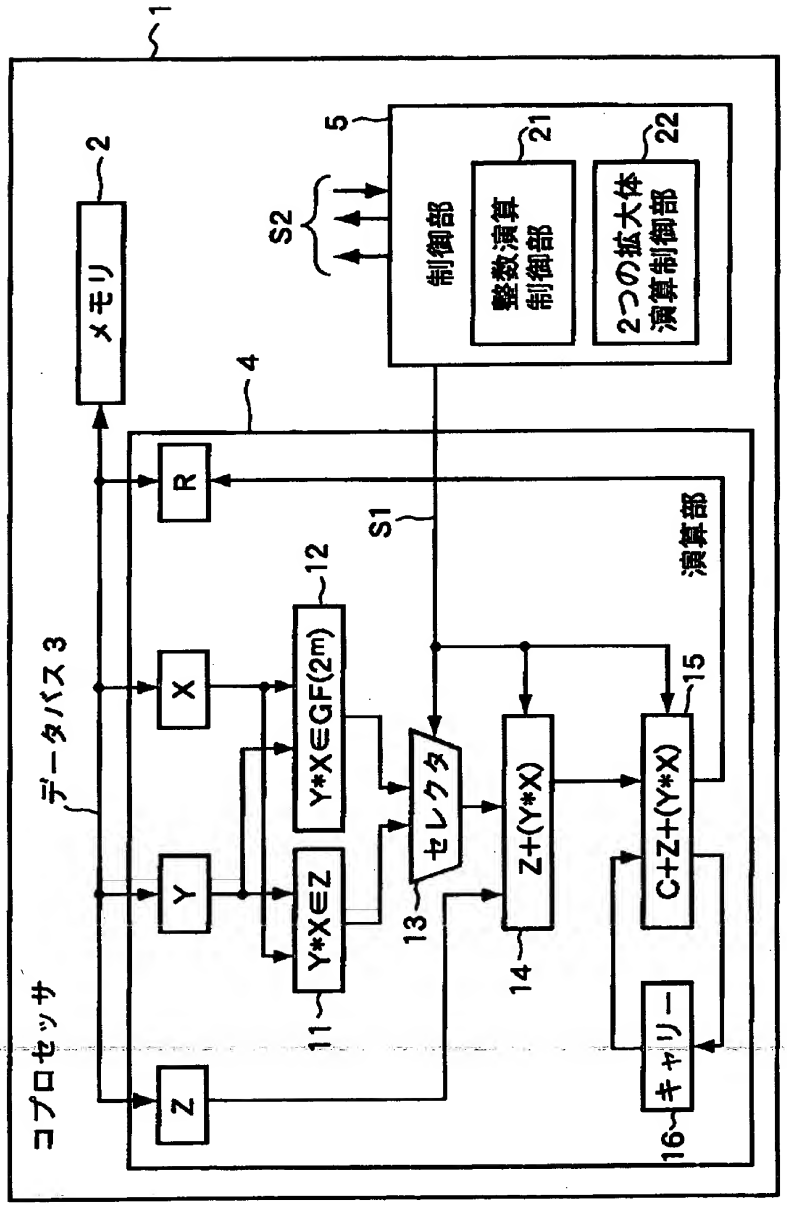
４１…乗算回路

４２，４３，４４…キャリー制御機能付き全加算器

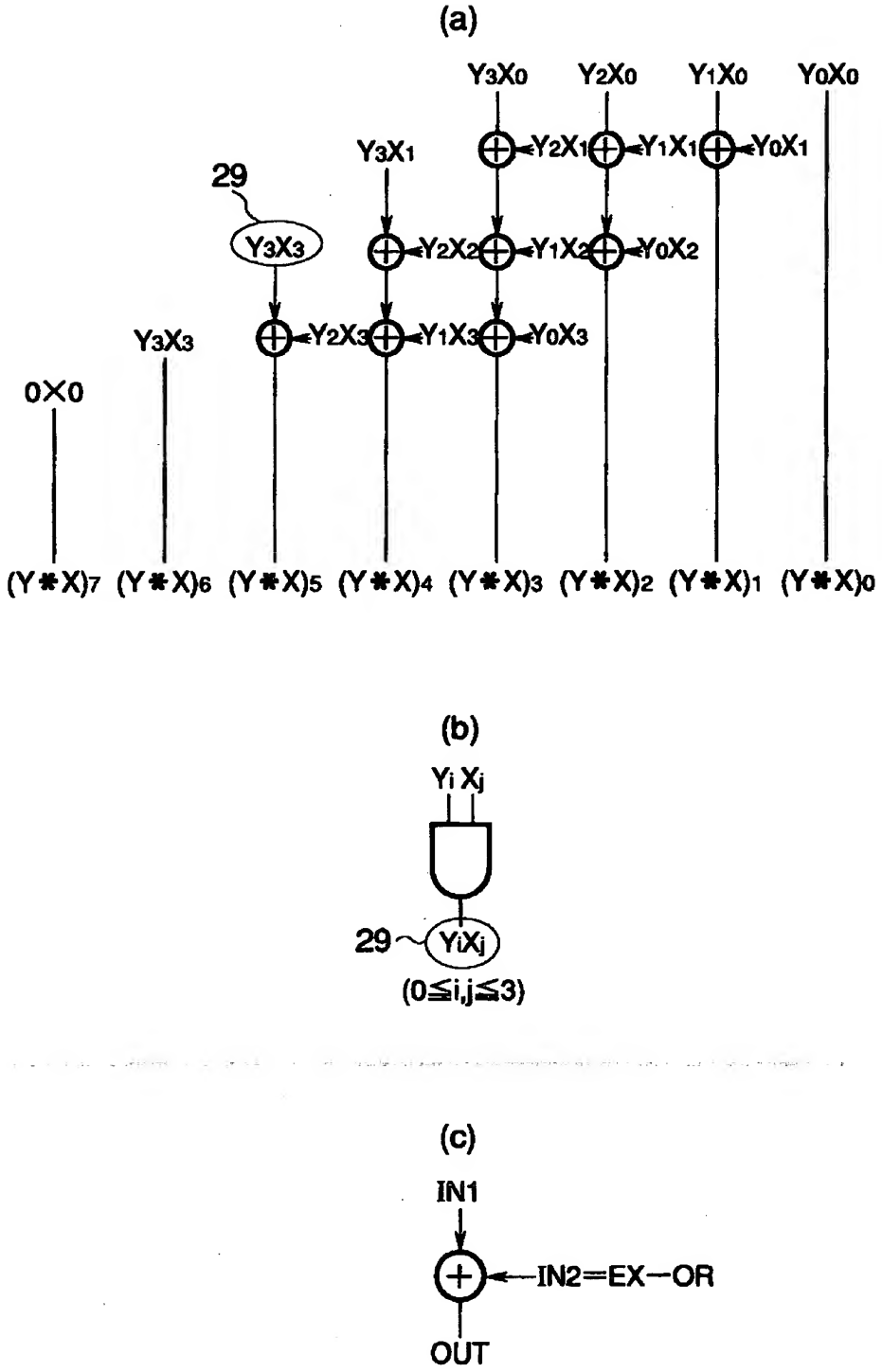
Ｓ１…制御信号

【書類名】　　図面

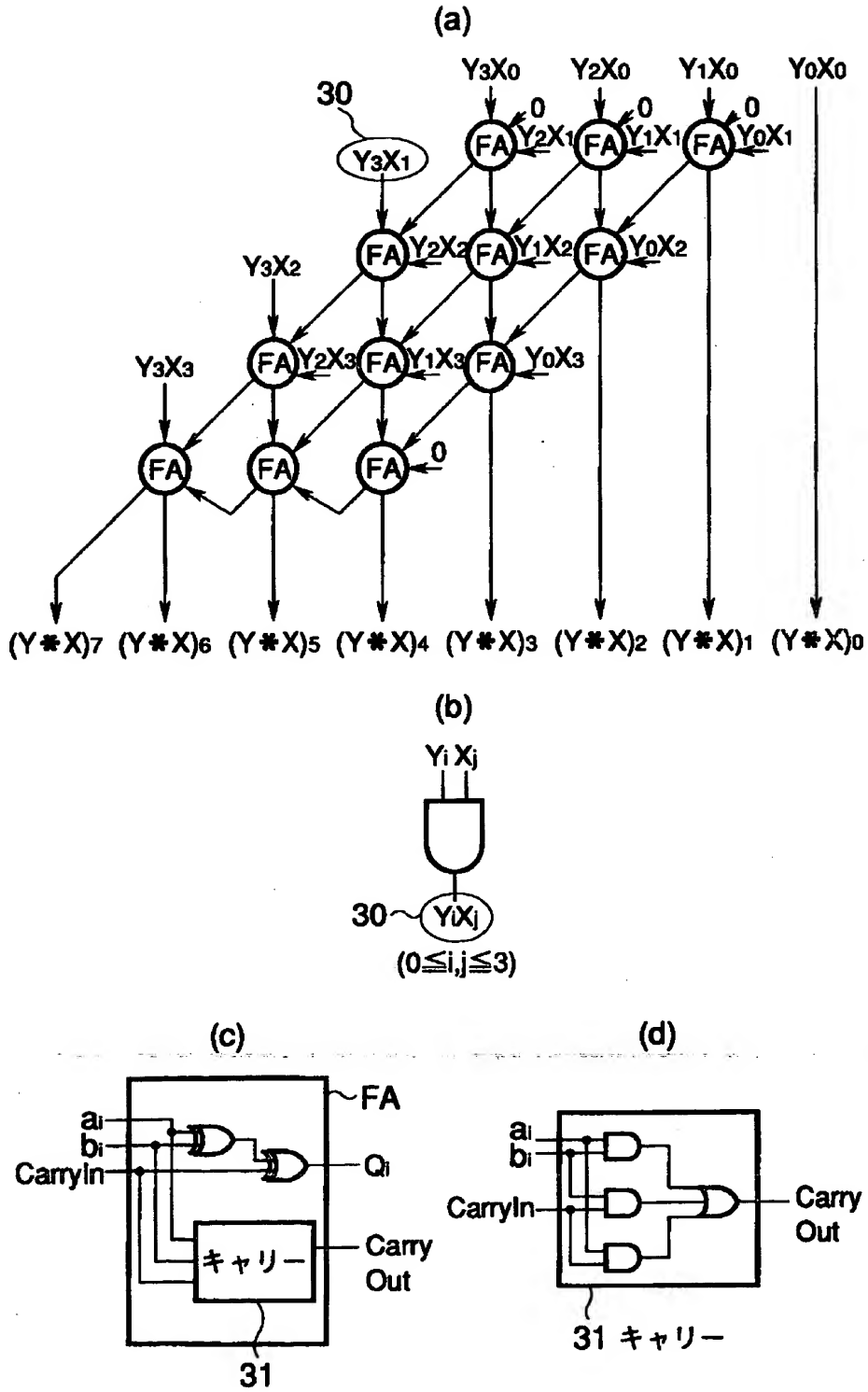
【図１】


1
2
メモリ
5
S2
制御部
21
整数演算制御部
22
2つの拡大体演算制御部
4
R
S1
演算部
データバス3
X
Y
Z
12
Y*X∈GF(2m)
Y*X∈Z
11
セレクタ
13
Z+(Y*X)
14
15
C+Z+(Y*X)
キャリー
16
コプロセッサ

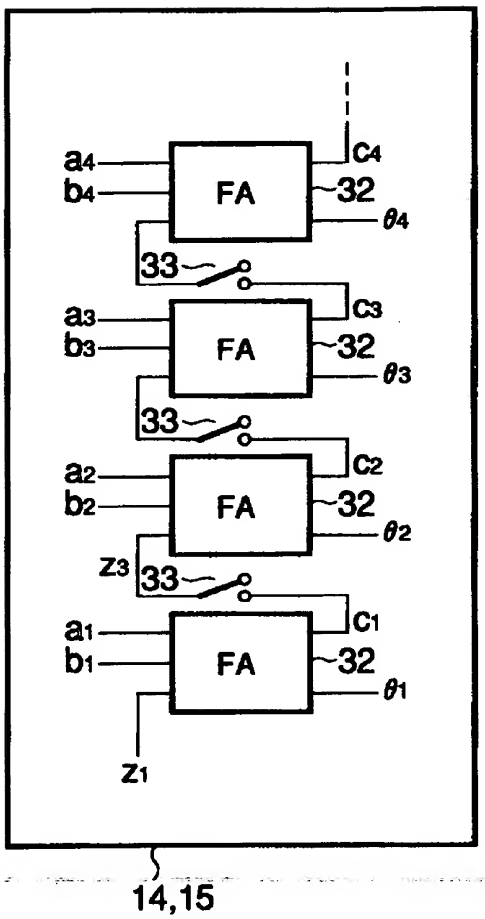
【図２】


(a)
Y3X0
Y2X0
Y1X0
Y0X0
Y3X1
Y2X1
Y1X1
Y0X1
29
Y3X3
Y2X2
Y1X2
Y0X2
Y3X3
Y2X3
Y1X3
Y0X3
0X0
(Y*X)7
(Y*X)6
(Y*X)5
(Y*X)4
(Y*X)3
(Y*X)2
(Y*X)1
(Y*X)0
(b)
Yi Xj
29
YiXj
(0≦i,j≦3)
(c)
IN1
IN2=EX−OR
OUT

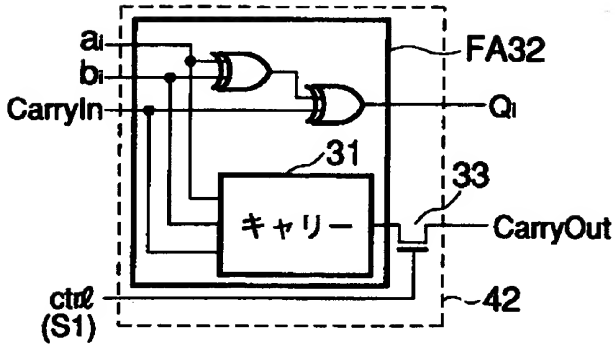
【図３】


(a)
Y3X0
Y2X0
Y1X0
Y0X0
30
Y3X1
FA
Y2X1
Y1X1
Y0X1
Y2X2
Y1X2
Y0X2
Y3X2
Y3X3
Y2X3
Y1X3
Y0X3
0
(Y*X)7
(Y*X)6
(Y*X)5
(Y*X)4
(Y*X)3
(Y*X)2
(Y*X)1
(Y*X)0
(b)
Yi Xj
30
YiXj
(0≦i,j≦3)
(c)
FA
ai
bi
CarryIn
Qi
キャリー
Carry
Out
31
(d)
ai
bi
CarryIn
Carry
Out
31 キャリー

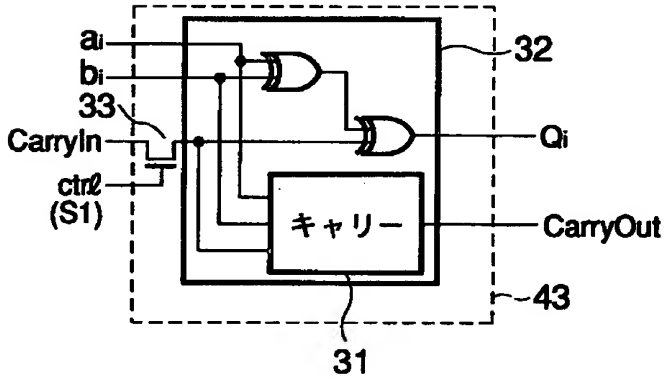
【図４】


a4
b4
FA
C4
32
θ4
33
a3
b3
FA
C3
32
θ3
33
a2
b2
FA
C2
32
θ2
z3
33
a1
b1
FA
C1
32
θ1
z1
14,15

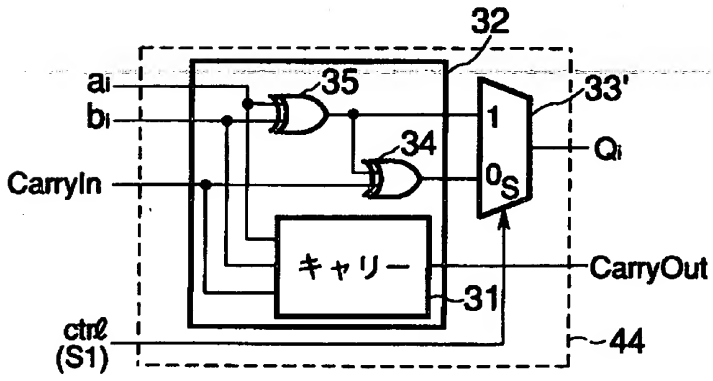
【図５】


ai
bi
CarryIn
FA32
Qi
31
33
キャリー
CarryOut
ctrl
(S1)
42

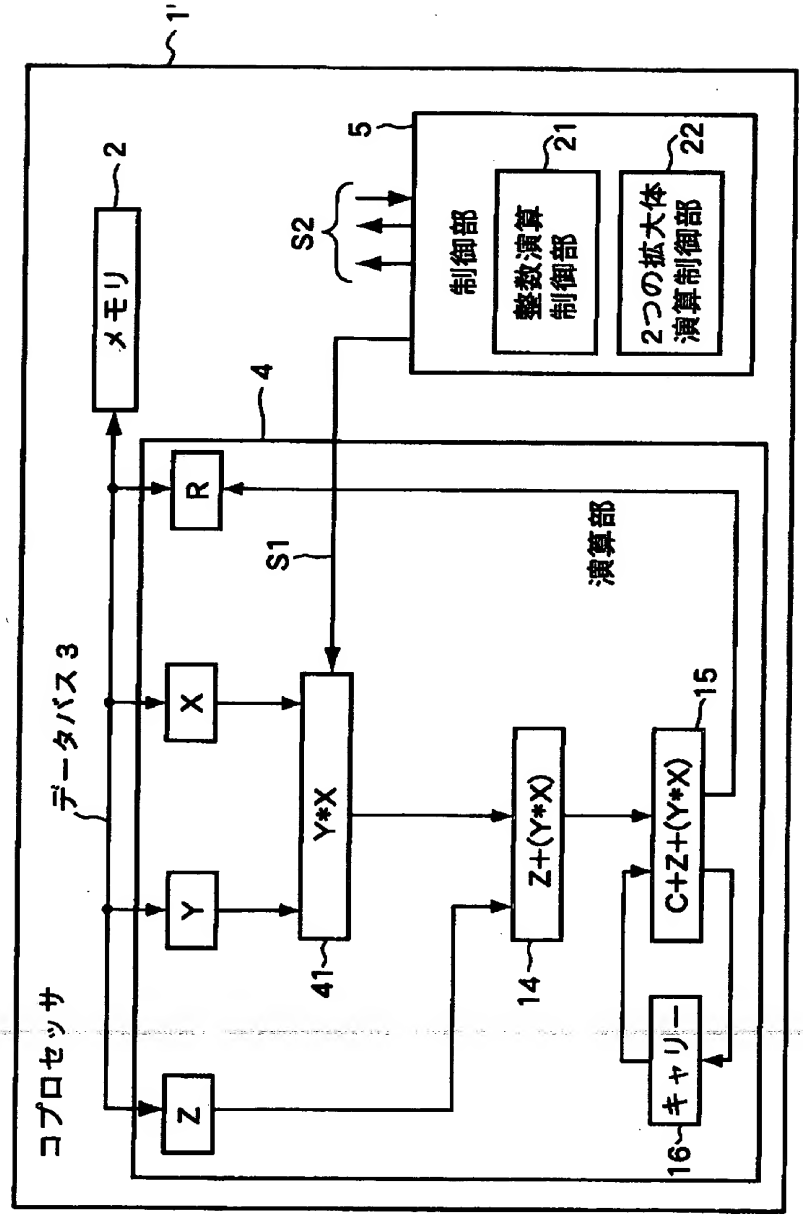
【図６】


ai
bi
33
CarryIn
ctrl
(S1)
32
Qi
キャリー
CarryOut
43
31

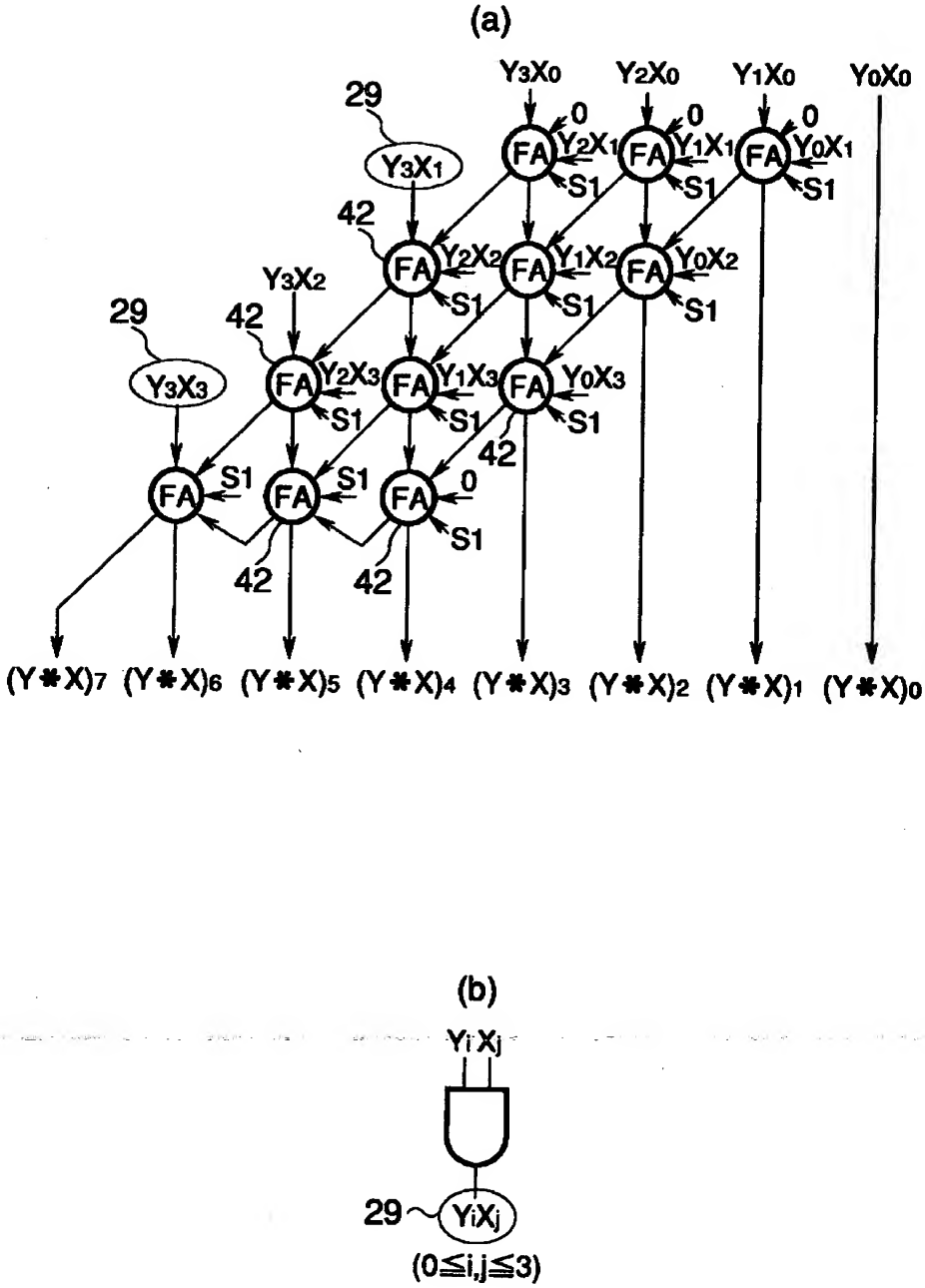
【図７】


32
ai
bi
35
33'
1
34
Qi
CarryIn
0
S
キャリー
CarryOut
31
ctrl
(S1)
44

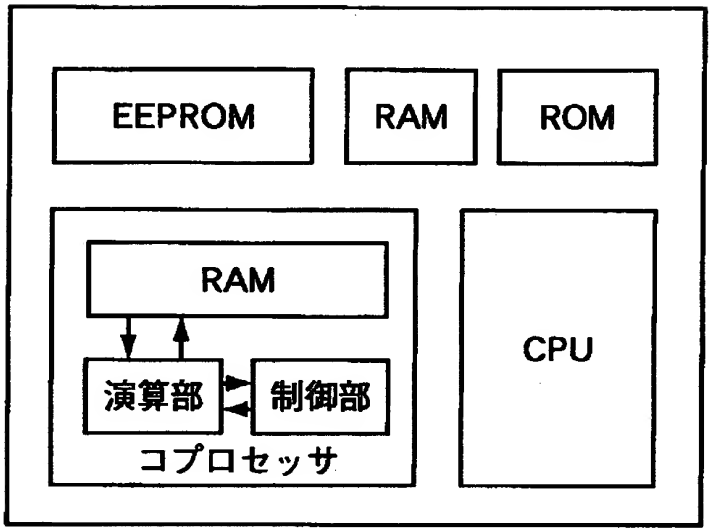
【図８】


1'
コプロセッサ
データバス 3
メモリ
2
制御部
5
整数演算制御部
21
2つの拡大体演算制御部
22
S2
4
演算部
R
S1
X
Y
Z
Y*X
41
Z+(Y*X)
14
C+Z+(Y*X)
15
キャリー
16

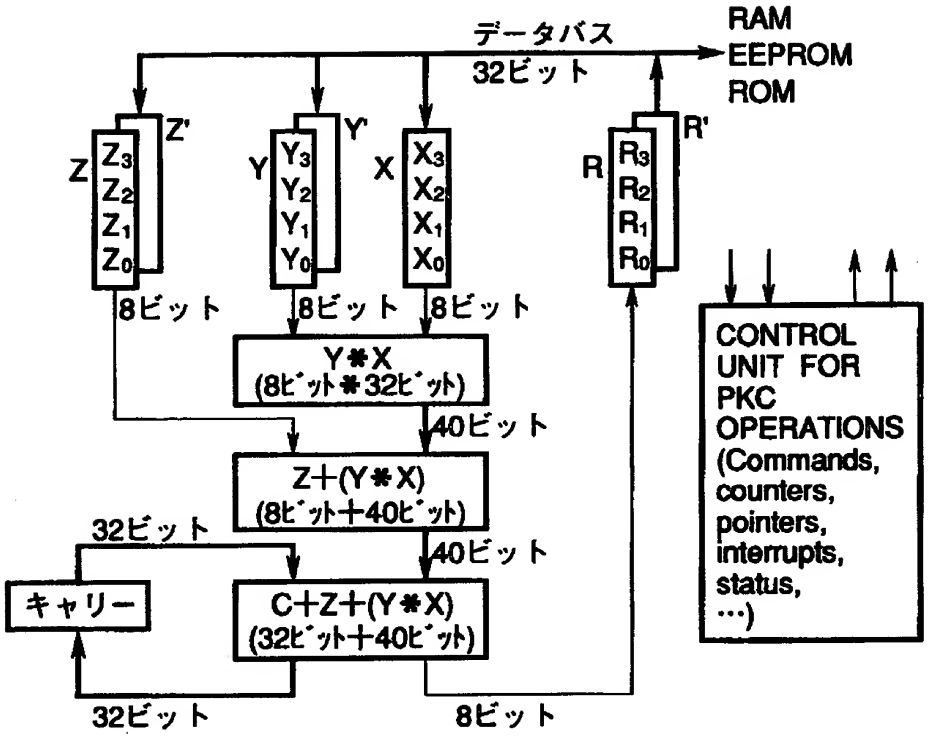
【図９】


(a)
Y3X0
Y2X0
Y1X0
Y0X0
29
Y3X1
FA
0
Y2X1
Y1X1
Y0X1
S1
42
Y2X2
Y1X2
Y0X2
Y3X2
Y3X3
Y2X3
Y1X3
Y0X3
(Y*X)7
(Y*X)6
(Y*X)5
(Y*X)4
(Y*X)3
(Y*X)2
(Y*X)1
(Y*X)0
(b)
YiXj
(0≦i,j≦3)

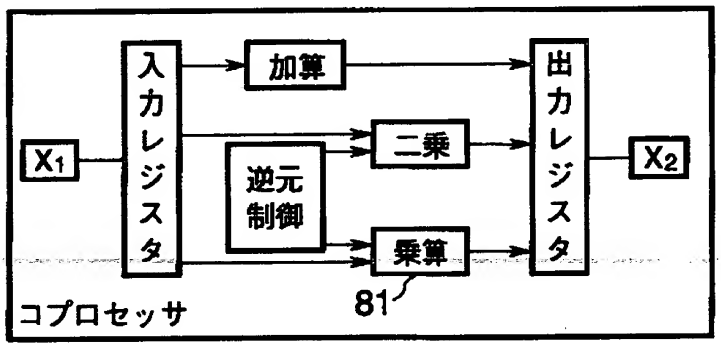
【図１０】



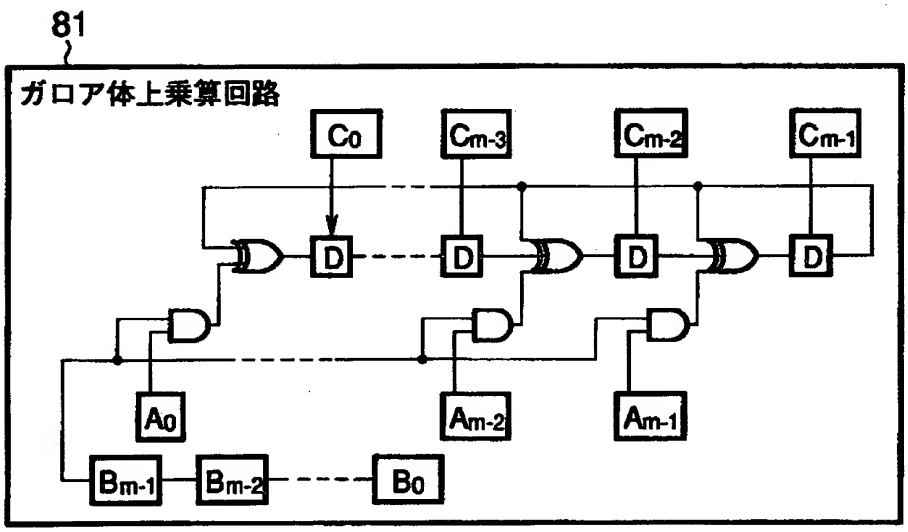
【図１１】


データバス
32ビット
RAM
EEPROM
ROM
Z
Z'
Y
Y'
X
R
R'
8ビット
8ビット
8ビット
Y*X
(8ビット*32ビット)
40ビット
Z+(Y*X)
(8ビット+40ビット)
32ビット
40ビット
キャリー
C+Z+(Y*X)
(32ビット+40ビット)
32ビット
8ビット
CONTROL
UNIT FOR
PKC
OPERATIONS
(Commands,
counters,
pointers,
interrupts,
status,
…)

【図１２】


入力レジスタ
加算
二乗
逆元制御
乗算
出力レジスタ
X1
X2
コプロセッサ
81

【図１３】



【書類名】　　要約書

【要約】

【課題】　本発明は、最小のアーキテクチャを追加するだけで整数型の演算に加えて２の拡大体上の演算をも実行できる。

【解決手段】　多倍長の積和演算装置１であって、整数型の単位乗算を実行する場合にはキャリーを伝搬させて単位乗算回路（１１，４１）を動作させ、２の拡大体の単位乗算を実行する場合にはキャリーを伝搬させずに単位乗算回路（１２，４１）を動作させるようにした演算装置。

【選択図】　　図１

出 願 人 履 歴 情 報

識別番号　〔０００００３０７８〕

１．変更年月日　１９９０年　８月２２日
［変更理由］　新規登録
住　所　神奈川県川崎市幸区堀川町７２番地
氏　名　株式会社東芝